



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/644,689	08/19/2003	Gregory Gordon Rose	020682	6710
23696	7590	11/01/2006	EXAMINER	
QUALCOMM INCORPORATED 5775 MOREHOUSE DR. SAN DIEGO, CA 92121			DADA, BEEMNET W	
		ART UNIT		PAPER NUMBER
				2135

DATE MAILED: 11/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/644,689	ROSE ET AL.
	Examiner Beemnet W. Dada	Art Unit 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 19 August 2003.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-53 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-53 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Ranhuze B. Tru
AU2135

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) Notice of Informal Patent Application
- 6) Other: _____

DETAILED ACTION

1. Claims 1-53 have been examined.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 37-43 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.
4. Claim 37 is directed to a medium for generating a key stream. The examiner respectfully asserts that the claim subject matter does not fall within the statutory class listed in 35 USC 101. Claim 37 is directed to functional descriptive material (i.e., computer program). Claims 37 is rejected as being directed to a computer program. Claims 38-43 depend from claim 37 and are rejected under the same rationale.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-53 are rejected under 35 U.S.C. 102(e) as being anticipated by Kim et al. US Pub 20050084112 A1 (hereinafter Kim).

7. As per claims 1, 27, 37 and 44, Kim teaches a method of generating a key stream comprising:

applying a cryptographic function on input values selected from a first array of values to generate output values (i.e., output values from registers 1050 and 1060 of figure 10, paragraph 0063);

selecting mask values from a second array of values (i.e., Masking sections 1000 to 1005 of figure 10, paragraph 0065-0066); and

combining the output values with the mask values to generate a key stream block for the key stream (i.e., secondary scrambling codes, figure 10, paragraphs 0065-0067).

wherein the first and second arrays are finite [see figure 10].

8. As per claims 2, 28, 38 and 45, Kim further teaches the method further comprising: generating the second array from the first array [figure 10 and paragraphs 0065-0067].

9. As per claims 3-5, Kim further teaches the method further comprising: using a linear feedback shift register (LFSR) to generate the first array, wherein the values of the first array correspond to the values of the LFSR states [figure 10 and paragraph 0063].

10. As per claims 6-8 and 29, Kim further teaches the method further comprising: applying the cryptographic function on updated input values selected from an updated first array of values to generate updated output values, selecting updated mask values from an updated second array of values, and combining the updated output values with the updated mask values

Art Unit: 2135

to generate a new key stream block for the key stream (i.e., at every period of the input clock, paragraphs 0063-0065).

11. As per claims 9, 30 and 46, Kim further teaches the method wherein the number of input values and the number of output values are equal [see figure 10].

12. As per claims 10 and 47, Kim further teaches the method wherein the first and second array each comprises seventeen values [see figure 10].

13. As per claim 11, 31 and 48, Kim further teaches the method wherein each value comprises of one or more words and wherein each word comprises two or more bytes [see figure 10].

14. As per claims 12-26, 32-36, 39-43 and 49-53, Kim further teaches the method wherein applying the cryptographic function comprises: performing a byte-wise substitution of at least one byte of an input value to generate primary intermediate values, and mixing at least two bytes of a primary intermediate value to generate a secondary intermediate value to generate the output values [see figure 10 and paragraphs 0063-0067].

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Beemnet W Dada

October 28, 2006

Beemnet W. Dada
AU2135